PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-318725
(43)Date of publication of application : 31.10.2002

(51)Int.Cl. G06F 12/14
G06F 3/06

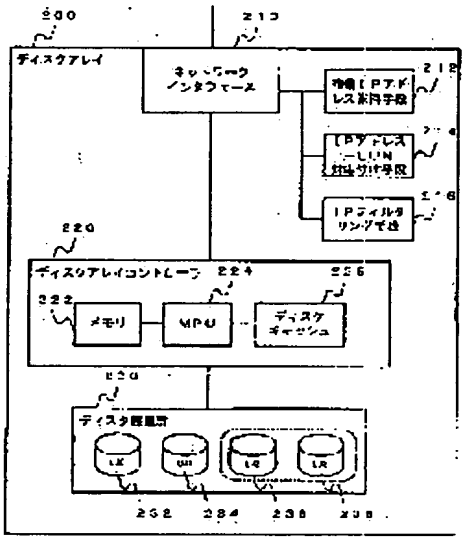
(21)Application number : 2001-121970
(22)Date of filing : 20.04.2001

(71)Applicant : HITACHI LTD
(72)Inventor : MANNEN AKIHIRO
YAGISAWA IKUYA
AJIMATSU YASUYUKI
MATSUNAMI NAOTO
MURAOKA KENJI

(54) DISK ARRAY SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a security function equal to a conventional LUN security in a disk array connected to a network by iSCSI technology.
SOLUTION: This system is provided with a means for holding a plurality of IP addresses inside the disk array, a means for making the IP address correspond to an LU, and a means for filtering transfer by watching the IP address to be used for transfer. Then the IP address is made correspond to the LU and the permission/no permission of transfer is set for every set IP addresses by a managing terminal, transfer, thus the filtering based on the IP address corresponding to the LU is realized on the disk array and a router.

図 2



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

* NOTICES *

CLAIMS

[Claim(s)]
[Claim 1] It is the disk array system which has two or more disk units arranged in the shape of an array. This disk array system The network interface which performs I/O with a host by iSCSI, The disk array controller which controls a disk array system, A means to hold two or more IP addresses, and the means which matches an IP address and Logical unit, It has a means to filter this transfer by the IP address used for a transfer. The disk array system characterized by for the directions from an administration terminal performing Logical unit and an IP address, and performing transfer filtering by the group of matching, a source IP address, and a destination IP address.
[Claim 2] The network system characterized by performing transfer filtering corresponding to Logical unit with the directions from this administration terminal in the network system equipped with the disk array system according to claim 1, the administration terminal which manages a disk array system, and the router which connects a network mutually by performing transfer filtering by the group of a source IP address and a destination IP address on a router.

[Translation done.]

* NOTICES *

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the access security of a disk array system especially mainly with respect to the control system for the disk array system used as a storage system of a computer system.
[0002]
[Description of the Prior Art] It is the storage which raised dependability by adding redundancy data to data while a disk array system is also called RAID (Redundant Arrays of Inexpensive Disks), takes the configuration which has arranged two or more disk units in the shape of an array and processes the lead demand (read-out demand of data) from a host, and a light demand (write request of data) at a high speed by juxtaposition actuation of a disk. A disk array system By the class and configuration of redundancy data It is classified into five level (paper:). ["A Case for Redundant Arrays of Inexpensive Disks(RAID)", David A.Patterson and Garsh Gibson and and Randy H.Katz, Computer Science DivisionDepartment of Electrical Engineering and Computer Sciences and Universityof CaliforniaBerkeley ACM SIGMOD pp.109-116 1988.
[0003] The disk array system is equipped with the disk group which consists of two or more disks. In order to realize the above disk arrays, it is necessary to change the read/write demand from a host into a read/write demand on each disk, to distribute data to each disk at the time of a light, and to perform data distribution / set control which gathers data from each disk at the time of a lead. Suppose that such control is called disk array control.
[0004] The read/write demand from a host is performed in the Logical unit unit generally called LU (Logical Unit).
[0005] The dedicated interface has been used in connection with a mainframe, and, as for the interface which connects a disk array with a host, SCSI (SmallComputer System Interface) and a fiber channel have been used by connection with an open system. However, the demand of wanting to connect storage is increasing in the network which spread explosively by the Internet in recent years using IP (Internet Protocol) as a protocol, the specification of iSCSI (Internet SCSI) which carries a SCSI protocol on IP is examined in IETF (Internet Engineering Task Force), and it will be draft-satran-iscsi-01.txt as Internet-Draft as of June, 2000. It is opened to the public.
[0006] With IP storage technique which makes iSCSI an example, if the direct continuation of a storage device becomes possible in IP network, the access nature to the storage device containing a disk array system will improve by leaps and bounds.
[0007]
[Problem(s) to be Solved by the Invention] By the iSCSI technique, direct continuation of the disk array system is carried out to IP network, and when the calculating machine on IP network to a disk array system becomes accessible simply, the opportunity of unlawful access will also increase so much, and the security function which prevents unlawful access becomes important.
[0008] When the host and the disk array system were connected in the network only for storage which consists of fiber channels and is called SAN (Storage Area Network), the security in data transfer was raised using the LUN security function in which consider that access from other

than the host who set up beforehand to a certain LU is unlawful access, and it is not received. About the LUN security function, it is indicated in JP,10-333839,A.
[0009] When a SCSI protocol is encapsulated inside IP, it becomes impossible however, to specify LU simply with an iSCSI technique only by seeing the packet of IP which flows a network top. In order to specify LU of an access place, and the host of an accessing agency, when it is necessary to analyze the packet of iSCSI of the TCP packet in an IP packet which is in inside further and a disk array system is connected to IP network by iSCSI, the technical problem that it becomes difficult to realize the same LUN security function as usual occurs.
[0010] Moreover, in IP network, various security functions are mounted in the router which interconnects each network. However, if those functions remain as they are, they cannot be used for the security of a disk array system, on the assumption that IP.
[0011] The purpose of this invention is to realize a security function equivalent to the conventional LUN security in the disk array connected to IP network using an IP address with an iSCSI technique.
[0012] Another purpose is in the thing of this invention for which a router realizes security equivalent to LUN security further, without adding a hand to the conventional router.
[0013]
[Means for Solving the Problem] In the array mold disc system which has two or more disk units which have arranged this invention on an array in order to attain said purpose The network interface which is connected to IP network and understands an iSCSI protocol, For the disk array controller which performs disk array control, in addition, a means to hold two or more IP addresses to one network interface, A means to match and manage LU inside an IP address and a disk array, and a means to judge whether the transfer is an unjust transfer by the group of the IP address of the source and the destination, and to filter based on a setup given beforehand are established.
[0014] Moreover, the function which carries out matching mapping of two or more IP addresses and LUs which the disk array other than a disk array function manager holds to the administration terminal which had managed the array mold disc system conventionally, and notifies a result to a disk array, and the function for which host to match whether it is accessible at which LU, to manage it on IP address level, and to set up the group of the IP address of LU with an accessible host at a network router or a disk array are prepared.
[0015] Thereby, since a disk array can know the group of the IP address of a just transfer, it can cancel the transfer by the group of inaccurate IP with a means to filter the unjust transfer prepared in the interior. Since LU is matched with the IP address, this is a security function equivalent to the conventional LUN security.
[0016] Similarly, since a network router can know the group of the IP address of a just transfer, it can cancel the transfer by the group of inaccurate IP by the function of packet filtering which it has from the former. Since LU is matched with the IP address, this is a security function equivalent to the conventional LUN security. It is effective in the ability to cancel the still more unjust transfer on the network router of the disk array exterior.
[0017]
[Embodiment of the Invention] Hereafter, the gestalt of operation of this invention is explained to a detail.
[0018] First, the configuration of the operation gestalt of this invention is explained using drawing 1 .
[0019] In drawing 1 , a host A100, a host B110, a host C120, and a host D130 are hosts who advance a read/write demand to a disk array 200, and output and input data. A disk array [in / in 200 / this invention], the router whose 300 is equipment which connects a network mutually, and 400 are the administration terminals of a network and a disk array 200. A network A500 and a network B510 are networks which became independent, respectively, and are mutually connected by the router 300. Although the host A100 and the host B110 exist on a network A500, they are accessible by minding a router 300 to the disk array 200 which exists on a network B510. A network A500 and a network B510 are networks which use IP as a protocol.
[0020] The internal-block Fig. of the disk array in this invention is shown in drawing 2 . The disk

array 200 is equipped with the network interface 210 which is connected to IP network and understands an iSCSI protocol, two or more IP address maintenance means 212, the IP address-LUN matching means 214, IP filtering means 216, the disk array controller 220, and the disk unit group 230. The disk array controller 220 is a part which performs disk array control including control of data I/O with a host, control of data division / integration peculiar to a disk array, and control of I/O of data with a disk unit group, and is equipped with the program ****** memory 222 which controls a disk array, MPU224 which performs a program and controls the whole disk array, and the disk cache 226 which buffers data transfer disk unit between groups with a host temporarily. The disk unit group 230 is constituted by two or more disk units allotted on the array.

[0021] In this operation gestalt, it shall have Logical unit LU 0-232, LU 1-234, LU 2-236, and LU 3-238 which were constituted by RAID of a simple substance disk or two or more disks.

[0022] Next, two or more IP address maintenance means 212 which is the description of this invention, the IP address-LUN matching means 214, and IP filtering means 216 are explained. Only one IP address was usually conventionally assigned to one network interface. This is because there were many network devices which do not support two or more IP addresses and it was difficult to assign and apply two or more IP addresses to one network interface. However, this problem is solved when IPv6 on condition of assigning two or more IP addresses to one network interface spreads. The disk array 200 of this invention makes it possible to assign two or more IP addresses to a network interface 210 by having two or more IP address maintenance means 212. The IP address-LUN matching means 214 matches the IP address which is a network identification child, and LUN (LU Number) which is the logical unit of disk accessing and is a substantial disk identifier. With this operation gestalt, a system administrator performs the matching of a what No. IP address is made to correspond to which LUN itself, and the result of matching is notified to the IP address-LUN matching means 214 through an administration terminal 400. This matching is managed with an IP address-LUN mapping table 500 like drawing 4 .

[0023] An example of matching of an IP address and LUN is shown in the IP address-LUN mapping table 500 of drawing 4 . Here, although it is a long digit string with the semantics as a network address properly speaking [an IP address], in this operation gestalt, an IP address shall be expressed as a digit string of 4 figures for explanation. In the IP address-LUN mapping table 500, IP address 510 and the LU number 520 are matched. the example expressed here -- an IP address -- "0000" and LU number -- "LU0" is matched and "0002" and "LU3" are similarly matched ["0001" and "LU1"] for "0002" and "LU2." Although LU2 and LU3 are matched with the same IP address"0002" here, and this is another LU as Logical unit, it is because it is the group of LU accessed on the conditions same in network, so the same IP address is assigned. Although LU2 consists of RAID1, high-speed access of it is attained, LU3 consists of RAID5 and this is accessed by the host with LU2 and LU3, when high-speed access is required, when LU is distinguished by the use application and LU2 accesses as LU3 is usually used, it is effective. [same]

[0024] The filtering function by the IP address which returns to drawing 2 , judges that IP filtering means 216 is a transfer unjust when it was the group to which one function in the packet-filtering function mounted in the usual router and an IP packet are investigated, and the group of a source IP address and a destination IP address is set beforehand and is the group which is not set up by making the transfer just, and repeals the transfer is realized. A system administrator sets the group of a just IP address as IP filtering means 216 through the IP address security setting up function 416 of an administration terminal 400.

[0025] The block diagram of the administration terminal 400 in this invention is shown in drawing 3 . Although the administration terminal 400 has the managed software 410 in the interior and realizes various managements by this, in addition to the disk array function manager 412 which it has conventionally in the managed software 410 in this operation gestalt, it is equipped with the IP address-LUN mapping function 414 and the IP address security setting up function 416. The disk array function manager 412 is a program which communicates with a disk array 200, gives support of LU creation, LU disconnection, etc., and manages a disk array 200. An IP address-

LUN mapping function has the IP address-LUN mapping table 500 shown in drawing 4 , and performs matching of actual IP address 510 and the LU number 520. Matching same as a disk array 200 is performed by telling matching of the IP address which the IP address-LUN mapping function 414 performed, and LU number to the IP address-LUN matching means of the disk array 200 interior. The IP address security setting up function 416 realizes the filtering function by the group of an IP address by having the table 600 corresponding to accessible LU as shown in drawing 5 , and setting the group of LU as a router 300 and IP filtering means 216 of the disk array 200 interior with the accessible host obtained from this table.

[0026] The table 600 corresponding to accessible LU shown in drawing 5 is a table with the item of IP address 640 corresponding to a host 610, host IP address 620 showing the host's IP address, accessible LU630 showing LU which can be accessed by the host, and LU showing the IP address corresponding to the LU. In the example of drawing 5 , Host A has IP address"0100" and shows the accessible thing to LU0 matched with IP address"0000." Host B is accessible to LU2 and LU3 which had IP address"0110" and were matched with IP address"0002" similarly. Thus, when a host is accessible to two or more LUs, the host will occupy two or more lines of a table.

[0027] Next, the actuation in this operation gestalt is explained. First, a system administrator uses the disk array function manager 412 of an administration terminal 400 at a certain host based on what access is predicted for what disk capacity from the need and which host, and a system design, specifies a RAID configuration, capacity, etc., and LU is created in a disk array 200. It differs from the former that a system administrator specifies the IP address which becomes an identifier at the time of accessing the LU from matching and a network in case LU is created here. The specified IP address is matched with LU by the IP address-LUN mapping function 414, and the matching is notified to the IP address-LUN matching means 214. Moreover, the matched IP address is notified to the host who accesses the LU. In case a host accesses the LU, he accesses the matched IP address by specifying it as the destination.

[0028] With this operation gestalt, four LUs, LU 0-232, LU 1-234, LU 2-236, and LU 3-238, are created, and suppose that IP address"0000", "0001", "0002", and "0002" are matched with each. This matching is expressed by the IP address-LUN mapping table 500 of drawing 4 . Although LU2 and LU3 are another LUs which consist of RAID1 and RAID5, since they are a group to which access equivalent in network is carried out, they are matched with the same IP address.

[0029] The IP address-LUN mapping function 414 and the IP address-LUN matching means 214 hold the IP address-LUN mapping table 500 inside.

[0030] With this operation gestalt, a host C120 shall access LU 1-234, LU 2-236, and LU 3-238, and a host D130 shall access [a host A100 / LU 0-232 / a host B110] LU 1-234 to LU 2-236 and LU 3-238. From here, the IP address security setting up function 416 creates the table 600 corresponding to accessible LU. A system administrator inputs the information which host accesses which LU. As shown in drawing 5 , a host's A100 IP address is "0100", "0110" and a host C120 have "0120" and, as for a host D130, a host B110 has the IP address of "0130." The system administrator knows beforehand a host's IP address accessed to a disk array 200. The table 600 corresponding to accessible LU means that access of the group of each line is permitted. The IP address security setting up function 416 Based on the table 600 corresponding to accessible LU, a router 300 and IP filtering means 216 are received. The transfer between IP address "0100" and "0000" (between hosts LU [A100 and] 0-232), The transfer between "0110" and "0002" (between hosts LU [B110 and] 2-236 and LU 3-238), The transfer between "0120" and "0001" (between hosts LU [C120 and] 1-234), It is specified that it permits "0120", and a transfer (between hosts LU [C120 and] 2-236 and LU 3-238) of a between and the transfer between "0002" "0130" and "0001" (between hosts LU [D130 and] 1-234). In addition, since both a host C120, a host D130, and the disk array 200 are on a network B510, a transfer in the meantime does not mind a router 300. Therefore, it is not necessary to specify that it grants a permission to a router 300 about the transfer between IP address "0120" and "0001", and "0120", and a transfer of a between and the transfer between "0002" "0130" and "0001."

[0031] Since the function which investigates the source IP address and destination IP address in an IP packet, and filters the unjust transfer which is not permitted is one function of packet filtering with which the conventional router is equipped, in this invention, a new function is unnecessary and extraordinarily [a router 300] usable in the conventional router.
[0032] By the above-mentioned setup, in case a host A100 accesses LU 0-232, the IP packet of source IP address"0100 "destination IP address" 0000" is used. Since it is set up so that the transfer between IP address "0100" and "0000" may grant a permission in a router 300, it is regarded as a just transfer, and similarly, it is judged with it being just also with IP filtering means 216 in a disk array 200, and the usual access processing is performed.
[0033] In order that it may carry out also here and a host B110 may access LU 0-232, supposing it uses the IP packet of source IP address"0110 "destination IP address" 0000", since a permission is not granted in a router 300, it will be regarded as an unjust transfer and the transfer between IP address "0110" and "0000" will be canceled.
[0034] In order that a host B110 may access LU 0-232, supposing it uses the IP packet of source IP address"0110 "destination IP address" 0002" Although a router 300 will let this inaccurate packet pass since it cannot recognize LU inside an IP packet but recognizes only an IP address Since it turns out that IP address"0002" and LU0 are not matched in the IP address-LUN mapping table 500 of the IP address-LUN matching means 214 in a disk array 200 In the disk array 200 interior, it can consider that this transfer is an unjust transfer, and it can be canceled.
[0035] In the disk array which is connected to IP network by the above configuration and actuation with an iSCSI technique according to this operation gestalt, a security function equivalent to the conventional LUN security is realizable with the group of the source IP address in an IP packet, and a destination IP address.
[0036] Moreover, in the router which connects a network mutually, a security function equivalent to the conventional LUN security is [the exterior of a disk array] realizable with the group of the same IP address.
[0037] Furthermore, from a host, since the same environment as I hear that it is visible to that there are two or more disk arrays and equivalence, it is and there are many disk arrays can be built by one disk array, it is effective in the unitary management of being attained and lowering the management cost of a disk array more cheaply, to match an IP address for every LU.
[0038] Furthermore, it is possible to shift the whole IP address which matched large LU of a load when shifting to another interface or another equipment, and from a host, after becomes accessible in the same environment and is henceforth effective in henceforth being easily realizable.
[0039] In addition, in this example, although the transfer of the management information from an administration terminal 400 to a disk array 200 and a router 300 is performed through the network B510, management information may be transmitted using the dedicated line 710 which connects a router 300 to the dedicated line 700 and administration terminal 400 which connect a disk array 200 to the administration terminal 400 instead of a network B510 as shown in drawing 6 . Dedicated lines 700 and 710 are realizable by for example, a serial communication line etc.
[0040] moreover, the IP address corresponding to LU 1-234 in this case although LU 1-234 is accessed in this example by only the host on a network B510 -- if "0001" is made into an effective local address only on a network B510, the data transfer of going away to an outer network through a router about LU 1-234 will be lost, and will serve as insurance in security.
[0041] Moreover, although the host explained in this example in the example which becomes an initiator and accesses a disk array, the data transfer from which the disk array became an initiator is also considered for the long distance backup through the Internet etc. In such a case, a security check can be carried [in / as well as this example / the data transfer from a disk array 200 to the equipment on an external network] out by filtering by the group of a transfer IP address on a router 300 by matching the IP address for initiators with LU for backup.
[0042] Moreover, although explained with this operation gestalt that the host had a single network interface, a host has two or more network interfaces, and even when using another IP address for each, it can realize similarly. Furthermore, when a host assigns two or more IP

addresses to one network interface and changes a usage for every IP address, as two or more hosts exist, it can realize.
[0043] Moreover, although it was explained with this operation gestalt that the disk array had a single network interface, even when a disk array has two or more network interfaces and uses another two or more IP addresses for each, it can realize similarly.
[0044] Moreover, although the IP address-LUN matching means 214 and IP filtering means 216 were formed in the disk array 200 with this operation gestalt, these may not be prepared but an applicable function may be realized by MPU224 and memory 222.
[0045]
[Effect of the Invention] A means by which two or more IP addresses can be held to the network interface of a disk array according to this invention as stated above, The means which matches LU and the IP address inside a disk array, and the means which looks at the group of the source IP address of an IP packet and a destination IP address, and can filter a transfer are established. It is supposed to a transfer of a host and LU that the IP address matched with LU is specified as a destination IP address, and is transmitted. When an administration terminal sets up the transfer [an IP address, mapping of LUN, and] of the group of which source IP address and destination IP address are permitted An unjust transfer can be canceled now by investigating the group of a source IP address and a destination IP address with a disk array and a router. The effectiveness that security equivalent to the LUN security conventional in the router top of the exterior of a disk array and a disk array is realizable is acquired.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is the network configuration Fig. of this invention.
[Drawing 2] It is the internal-block Fig. of the disk array in this invention.
[Drawing 3] It is the internal-block Fig. of the administration terminal in this invention.
[Drawing 4] It is drawing showing the mapping table of an IP address and LUN.
[Drawing 5] It is drawing in which a host shows the table of accessible LU.
[Drawing 6] It is the network configuration Fig. of another configuration.
[Description of Notations]
100 [— Host D, 200 / — A disk array, 300 / — A router, 400 / — An administration terminal, 210 / — A network interface, 212 / — Two or more IP address maintenance means, 214 / — An IP address-LUN matching means, 216 / — IP filtering means.] — Host A, 110 — Host B, 120 — Host C, 130

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－318725
（P2002－318725A）
(43)公開日　平成14年10月31日(2002.10.31)

(51)Int.Cl.'	識別記号	ＦＩ	テーマコード'（参考）
Ｇ０６Ｆ　12/14	３１０	Ｇ０６Ｆ　12/14	３１０Ｋ　５Ｂ０１７
3/06	３０４	3/06	３０４Ｈ　５Ｂ０６５
	５４０		５４０

審査請求　未請求　請求項の数２　ＯＬ　（全９頁）

(21)出願番号　特願2001－121970(P2001－121970)

(22)出願日　平成13年４月20日(2001.4.20)

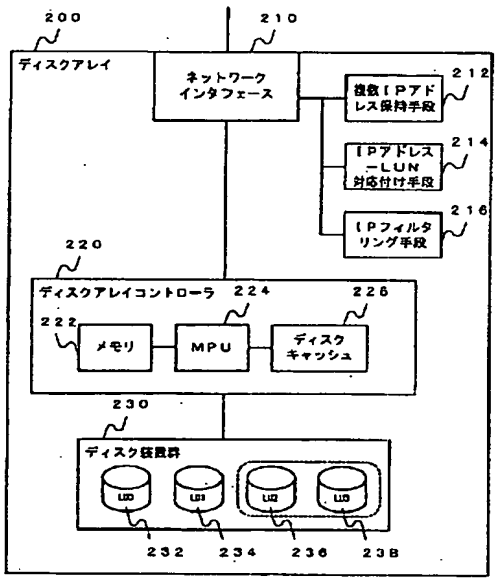
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　萬年　暁弘
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　八木沢　育哉
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(74)代理人　100075096
弁理士　作田　康夫

最終頁に続く

(54)【発明の名称】　ディスクアレイシステム

(57)【要約】
【課題】ｉＳＣＳＩ技術でネットワークに接続されるディスクアレイにおいて、従来のＬＵＮセキュリティと同等のセキュリティ機能を実現する。
【解決手段】ディスクアレイ内部に複数のＩＰアドレスを保持する手段と、ＩＰアドレスとＬＵを対応付ける手段と、転送に使われるＩＰアドレスを見て転送をフィルタリングする手段を設け、管理端末によりＩＰアドレスとＬＵの対応付け、およびＩＰアドレスの組による転送の許可／不許可を設定することにより、ディスクアレイおよびルータ上でＬＵに対応するＩＰアドレスによる転送フィルタリングを実現する。

図２



【特許請求の範囲】

【請求項１】　アレイ状に配置した複数のディスク装置を有するディスクアレイシステムであって、該ディスクアレイシステムは、ｉＳＣＳＩによりホストとの入出力を行うネットワークインタフェースと、ディスクアレイシステムを制御するディスクアレイコントローラと、複数のＩＰアドレスを保持する手段と、ＩＰアドレスと論理ユニットを対応付ける手段と、転送に使われるＩＰアドレスにより該転送をフィルタリングする手段を備え、管理端末からの指示により論理ユニットとＩＰアドレスを対応付け、転送元ＩＰアドレスと転送先ＩＰアドレスの組により転送フィルタリングを行うことを特徴とするディスクアレイシステム。

【請求項２】　請求項１記載のディスクアレイシステムと、ディスクアレイシステムを管理する管理端末と、ネットワークを相互に接続するルータとを備えたネットワークシステムにおいて、該管理端末からの指示によりルータ上で転送元ＩＰアドレスと転送先ＩＰアドレスの組により転送フィルタリングを行うことにより、論理ユニットに対応した転送フィルタリングを行うことを特徴とするネットワークシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は主として、コンピュータシステムの記憶システムとして用いられるディスクアレイシステムのための制御方式に係わり、特にディスクアレイシステムのアクセスセキュリティに関する。

【０００２】

【従来の技術】ディスクアレイシステムは、ＲＡＩＤ（Redundant Arrays of Inexpensive Disks）とも呼ばれ、複数のディスク装置をアレイ状に配置した構成をとり、ホストからのリード要求（データの読み出し要求）およびライト要求（データの書き込み要求）をディスクの並列動作によって高速に処理するとともに、データに冗長データを付加することによって信頼性を向上させた記憶装置である。ディスクアレイシステムは、冗長データの種類と構成により５つのレベルに分類されている（論文："A Case for Redundant Arrays of Inexpensive Disks(RAID)", David A. Patterson, Garsh Gibson, and Randy H. Katz, Computer Science DivisionDepartment of Electrical Engineering and Computer Sciences, Universityof California Berkeley ACM SIGMOD pp. 109－116 1988）。

【０００３】ディスクアレイシステムは複数のディスクからなるディスク群を備えている。上記のようなディスクアレイを実現するためには、ホストからのリード／ライト要求を各ディスクへのリード／ライト要求に変換し、ライト時にはデータを各ディスクへ分散し、リード時には各ディスクからデータを集合するデータ分散・集合制御を行う必要がある。このような制御をディスクアレイ制御と呼ぶこととする。

【０００４】ホストからのリード／ライト要求は、一般的にＬＵ（Logical Unit）と呼ばれる論理ユニット単位で行われる。

【０００５】ホストとディスクアレイを接続するインタフェースは、メインフレームとの接続では専用インタフェースが、オープンシステムとの接続ではＳＣＳＩ（SmallComputer System Interface）やファイバチャネルが用いられてきた。ところが、近年インターネットにより爆発的に普及した、ＩＰ（Internet Protocol）をプロトコルとして用いたネットワークでストレージを接続したいという要求が高まっており、ＩＰ上にＳＣＳＩのプロトコルを載せるｉＳＣＳＩ（Internet SCSI）という規格がＩＥＴＦ（Internet Engineering Task Force）において検討され、２０００年６月の時点でInternet－Draftとしてdraft－satran－iscsi－01.txt が公開されている。

【０００６】ｉＳＣＳＩを一例とするＩＰストレージ技術により、ＩＰネットワークにストレージデバイスが直接接続可能になると、ディスクアレイシステムを含むストレージデバイスへのアクセス性は飛躍的に向上する。

【０００７】

【発明が解決しようとする課題】ｉＳＣＳＩ技術により、ＩＰネットワークにディスクアレイシステムが直接接続され、ＩＰネットワーク上の計算機からディスクアレイシステムが簡単にアクセス可能になると、それだけ不正アクセスの機会も増大することとなり、不正アクセスを防ぐセキュリティ機能が重要となる。

【０００８】ファイバチャネルで構成されＳＡＮ（Storage Area Network）と呼ばれるストレージ専用のネットワークでホストおよびディスクアレイシステムが接続されていた時には、あるＬＵに対してあらかじめ設定しておいたホスト以外からのアクセスを不正アクセスとみなして受け付けないＬＵＮセキュリティ機能を使用してデータ転送におけるセキュリティを高めていた。ＬＵＮセキュリティ機能については、特開平１０－３３３８３９号公報において開示されている。

【０００９】ところが、ｉＳＣＳＩ技術により、ＳＣＳＩのプロトコルがＩＰの内部にカプセル化されてしまうと、ネットワーク上を流れるＩＰのパケットを見ただけでは単純にＬＵを特定することができなくなる。アクセス先のＬＵおよびアクセス元のホストを特定する為には、ＩＰパケットの中にあるＴＣＰパケットのさらに中にあるｉＳＣＳＩのパケットを解析する必要があり、ｉＳＣＳＩによってディスクアレイシステムをＩＰネットワークに接続した場合、従来と同様のＬＵＮセキュリティ機能を実現するのが難しくなるという課題がある。

【００１０】また、ＩＰネットワークでは、各ネットワークを相互接続するルータにさまざまなセキュリティ機能が実装されている。しかしながらそれらの機能はＩＰ

を前提としたものであり、そのままではディスクアレイシステムのセキュリティに使用することはできない。

【００１１】本発明の目的は、ｉＳＣＳＩ技術でＩＰネットワークに接続されるディスクアレイにおいて、ＩＰアドレスを用いて従来のＬＵＮセキュリティと同等のセキュリティ機能を実現することにある。

【００１２】本発明のさらにもう１つの目的は、従来のルータに手を加えることなく、ルータでＬＵＮセキュリティと同等のセキュリティを実現することにある。

【００１３】

【課題を解決するための手段】前記目的を達成する為に、本発明は、アレイ上に配置した複数のディスク装置を有するアレイ型ディスクシステムにおいて、ＩＰネットワークに接続されｉＳＣＳＩプロトコルを解するネットワークインタフェースと、ディスクアレイ制御を行うディスクアレイコントローラに加えて、１つのネットワークインタフェースに複数のＩＰアドレスを保持する手段と、ＩＰアドレスとディスクアレイ内部のＬＵを対応付けて管理する手段と、あらかじめ与えられた設定に基づき転送元と転送先のＩＰアドレスの組によりその転送が不正な転送であるかを判断しフィルタリングする手段を設ける。

【００１４】また、従来アレイ型ディスクシステムを管理していた管理端末に、ディスクアレイ管理機能の他に、ディスクアレイが保持する複数のＩＰアドレスとＬＵとを対応付けマッピングし結果をディスクアレイに通知する機能と、どのホストがどのＬＵにアクセス可能であるかを対応付け、それをＩＰアドレスレベルで管理し、アクセス可能であるホストとＬＵのＩＰアドレスの組をネットワークルータやディスクアレイに設定する機能を設ける。

【００１５】これによりディスクアレイは、正当な転送のＩＰアドレスの組を知ることができるので、内部に設けた不正な転送をフィルタリングする手段により、不正なＩＰの組による転送を破棄することができる。ＬＵをＩＰアドレスと対応付けているので、これは従来のＬＵＮセキュリティと同等のセキュリティ機能である。

【００１６】同様にネットワークルータは、正当な転送のＩＰアドレスの組を知ることができるので、従来から持っているパケットフィルタリングの機能により、不正なＩＰの組による転送を破棄することができる。ＬＵをＩＰアドレスと対応付けているので、これは従来のＬＵＮセキュリティと同等のセキュリティ機能である。さらにディスクアレイ外部のネットワークルータ上で不正な転送を破棄することができるという効果がある。

【００１７】

【発明の実施の形態】以下、本発明の実施の形態を、詳細に説明する。

【００１８】まず、本発明の実施形態の構成を図１を用いて説明する。

【００１９】図１において、ホストＡ１００、ホストＢ１１０、ホストＣ１２０、ホストＤ１３０は、ディスクアレイ２００に対してリード／ライト要求を出し、データの入出力を行うホストである。２００は本発明におけるディスクアレイ、３００はネットワークを相互に接続する装置であるルータ、４００はネットワークおよびディスクアレイ２００の管理端末である。ネットワークＡ５００とネットワークＢ５１０はそれぞれ独立したネットワークであり、ルータ３００により相互に接続されている。ホストＡ１００およびホストＢ１１０は、ネットワークＡ５００上に存在しているが、ルータ３００を介することにより、ネットワークＢ５１０上に存在するディスクアレイ２００へアクセス可能となっている。ネットワークＡ５００とネットワークＢ５１０は、プロトコルとしてＩＰを用いるネットワークである。

【００２０】図２に本発明におけるディスクアレイの内部ブロック図を示す。ディスクアレイ２００は、ＩＰネットワークに接続されｉＳＣＳＩプロトコルを解するネットワークインタフェース２１０と、複数ＩＰアドレス保持手段２１２と、ＩＰアドレス－ＬＵＮ対応付け手段２１４と、ＩＰフィルタリング手段２１６と、ディスクアレイコントローラ２２０と、ディスク装置群２３０とを備えている。ディスクアレイコントローラ２２０は、ホストとのデータ入出力の制御、ディスクアレイ特有のデータ分割／統合の制御、ディスク装置群とのデータの入出力の制御を含むディスクアレイ制御を行う部位であり、ディスクアレイを制御するプログラム蓄えるメモリ２２２と、プログラムを実行しディスクアレイ全体の制御を行うＭＰＵ２２４と、ホストとディスク装置群間のデータ転送を一時バッファリングするディスクキャッシュ２２６とを備えている。ディスク装置群２３０は、アレイ上に配された複数ディスク装置によって構成されている。

【００２１】本実施形態においては、単体ディスクあるいは複数ディスクのＲＡＩＤにより構成された論理ユニットＬＵ０－２３２、ＬＵ１－２３４、ＬＵ２－２３６、ＬＵ３－２３８を備えるものとする。

【００２２】次に、本発明の特徴である複数ＩＰアドレス保持手段２１２、ＩＰアドレス－ＬＵＮ対応付け手段２１４、ＩＰフィルタリング手段２１６について説明する。従来は通常、一つのネットワークインタフェースには一つのＩＰアドレスのみを割り当てていた。これは、複数ＩＰアドレスに対応していないネットワーク機器が多く、一つのネットワークインタフェースに複数のＩＰアドレスを割り当てて運用することが難しかったためである。しかしながら、一つのネットワークインタフェースに複数のＩＰアドレスを割り当てることを前提とするＩＰｖ６が普及することにより、この問題は解消される。本発明のディスクアレイ２００は、複数ＩＰアドレス保持手段２１２を持つことにより、ネットワークイン

タフェース２１０に複数のＩＰアドレスを割り当てることを可能としている。ＩＰアドレス－ＬＵＮ対応付け手段２１４は、ネットワーク識別子であるＩＰアドレスと、ディスクアクセスの論理的な単位であり実質的なディスク識別子であるＬＵＮ（ＬＵ Ｎｕｍｂｅｒ）の対応付けを行う。本実施形態では、ＩＰアドレス何番をどのＬＵＮに対応させるかという対応付け自体はシステム管理者が行い、管理端末４００を介して対応付けの結果がＩＰアドレス－ＬＵＮ対応付け手段２１４に通知される。この対応付けは、図４のようなＩＰアドレス－ＬＵＮマッピングテーブル５００をもって管理される。

【００２３】ＩＰアドレスとＬＵＮの対応付けの一例を図４のＩＰアドレス－ＬＵＮマッピングテーブル５００に示す。ここで、ＩＰアドレスは本来ならばネットワークアドレスとしての意味を持った長い数字列であるが、本実施形態においては説明のために４桁の数字列としてＩＰアドレスを表すものとする。ＩＰアドレス－ＬＵＮマッピングテーブル５００では、ＩＰアドレス５１０とＬＵ番号５２０を対応付けている。ここに表されている例では、ＩＰアドレス”００００”とＬＵ番号”ＬＵ０”が対応付けられ、同様に”０００１”と”ＬＵ１”が、”０００２”と”ＬＵ２”が、”０００２”と”ＬＵ３”が対応付けられている。ここでＬＵ２とＬＵ３は同じＩＰアドレス”０００２”に対応付けられているが、これは論理ユニットとしては別のＬＵであるが、ネットワーク的には同じ条件でアクセスされるＬＵの組であるため、同じＩＰアドレスを割り振っているからである。これは例えば、ＬＵ２がＲＡＩＤ１で構成され高速なアクセスが可能となっており、ＬＵ３がＲＡＩＤ５で構成されていて、ＬＵ２、ＬＵ３ともに同じホストからアクセスされるが高速なアクセスが必要な時はＬＵ２が、通常はＬＵ３が使用されるというように使用用途によりＬＵを区別してアクセスするような場合に有効である。

【００２４】図２に戻って、ＩＰフィルタリング手段２１６は、通常のルータに実装されているパケットフィルタリング機能の内の一機能、ＩＰパケットを調べ転送元ＩＰアドレスと転送先ＩＰアドレスの組があらかじめ設定されている組であればその転送を正当なものとし、設定されていない組であった場合には不正な転送であると判断してその転送を無効とする、ＩＰアドレスによるフィルタリング機能を実現する。正当なＩＰアドレスの組は、システム管理者が管理端末４００のＩＰアドレスセキュリティ設定機能４１６を介してＩＰフィルタリング手段２１６に設定する。

【００２５】図３に、本発明における管理端末４００のブロック図を示す。管理端末４００は、内部に管理ソフト４１０を持っており、これによってさまざまな管理を実現するが、本実施形態においては管理ソフト４１０内に従来持っているディスクアレイ管理機能４１２に加えて、ＩＰアドレス－ＬＵＮマッピング機能４１４、ＩＰアドレスセキュリティ設定機能４１６を備える。ディスクアレイ管理機能４１２は、ディスクアレイ２００と通信し、ＬＵ作成やＬＵ開放等の支持を与えてディスクアレイ２００を管理するプログラムである。ＩＰアドレス－ＬＵＮマッピング機能は、図４に示すＩＰアドレス－ＬＵＮマッピングテーブル５００を持ち、実際のＩＰアドレス５１０とＬＵ番号５２０の対応付けを行う。ＩＰアドレス－ＬＵＮマッピング機能４１４が行ったＩＰアドレスとＬＵ番号の対応付けを、ディスクアレイ２００内部のＩＰアドレス－ＬＵＮ対応付け手段に伝えることにより、ディスクアレイ２００でも同じ対応付けが行われる。ＩＰアドレスセキュリティ設定機能４１６は、図５に示すようなアクセス可能ＬＵ対応テーブル６００を持ち、このテーブルから得られるアクセス可能なホストとＬＵの組をルータ３００およびディスクアレイ２００内部のＩＰフィルタリング手段２１６に設定することにより、ＩＰアドレスの組によるフィルタリング機能を実現する。

【００２６】図５に示すアクセス可能ＬＵ対応テーブル６００は、ホスト６１０、そのホストのＩＰアドレスを表すホストＩＰアドレス６２０、そのホストがアクセスすることが可能なＬＵを表すアクセス可能ＬＵ６３０、そのＬＵに対応するＩＰアドレスを表すＬＵ対応ＩＰアドレス６４０の項目を持つテーブルである。図５の例では、ホストＡはＩＰアドレス”０１００”を持ち、ＩＰアドレス”００００”に対応付けられたＬＵ０にアクセス可能であることを示している。同様にホストＢはＩＰアドレス”０１１０”を持ち、ＩＰアドレス”０００２”に対応付けられたＬＵ２およびＬＵ３にアクセス可能である。このようにホストが複数のＬＵにアクセス可能の場合は、そのホストがテーブルの複数の行を占めることになる。

【００２７】次に、本実施形態における動作について説明する。まず初めに、システム管理者が、あるホストにはどのくらいのディスク容量が必要か、どのホストからどのくらいのアクセスが予測されるか等のシステム設計を元に、管理端末４００のディスクアレイ管理機能４１２を用いて、ＲＡＩＤ構成、容量等を指定して、ディスクアレイ２００内にＬＵを作成する。ここで従来と異なるのは、システム管理者はＬＵを作成する際にそのＬＵに対応付け、ネットワークからアクセスする際の識別子になるＩＰアドレスを指定することである。指定されたＩＰアドレスはＩＰアドレス－ＬＵＮマッピング機能４１４によりＬＵと対応付けられ、ＩＰアドレス－ＬＵＮ対応付け手段２１４にその対応付けが通知される。また、そのＬＵをアクセスするホストに対して、対応付けたＩＰアドレスが通知される。ホストはそのＬＵをアクセスする際には、対応付けられたＩＰアドレスを転送先に指定してアクセスを行う。

【００２８】本実施形態では、ＬＵ０－２３２、ＬＵ１－２３４、ＬＵ２－２３６、ＬＵ３－２３８の４つのＬＵを作成し、それぞれにＩＰアドレス”０００”、”０００１”、”０００２”、”０００２”を対応付けることとする。この対応付けは、図４のＩＰアドレス－ＬＵＮマッピングテーブル５００に表される。ＬＵ２とＬＵ３は例えばＲＡＩＤ１とＲＡＩＤ５で構成される別ＬＵであるが、ネットワーク的には同等のアクセスがされる組であるため、同じＩＰアドレスに対応付けている。

【００２９】ＩＰアドレス－ＬＵＮマッピングテーブル５００は、ＩＰアドレス－ＬＵＮマッピング機能４１４およびＩＰアドレス－ＬＵＮ対応付け手段２１４が内部に保持する。

【００３０】本実施形態では、ホストＡ１００がＬＵ０－２３２を、ホストＢ１１０がＬＵ２－２３６とＬＵ３－２３８とを、ホストＣ１２０がＬＵ１－２３４とＬＵ２－２３６とＬＵ３－２３８とを、ホストＤ１３０がＬＵ１－２３４をアクセスするものとする。ここから、ＩＰアドレスセキュリティ設定機能４１６は、アクセス可能ＬＵ対応テーブル６００を作成する。どのホストがどのＬＵをアクセスするかという情報は、システム管理者が入力する。図５に示されるように、ホストＡ１００のＩＰアドレスは”０１００”であり、ホストＢ１１０は”０１１０”、ホストＣ１２０は”０１２０”、ホストＤ１３０は”０１３０”のＩＰアドレスを持つ。システム管理者は、ディスクアレイ２００へアクセスするホストのＩＰアドレスをあらかじめ知っている。アクセス可能ＬＵ対応テーブル６００は、各行の組のアクセスが許可されていることを表している。ＩＰアドレスセキュリティ設定機能４１６は、アクセス可能ＬＵ対応テーブル６００を元に、ルータ３００とＩＰフィルタリング手段２１６に対して、ＩＰアドレス”０１００”と”０００”間の転送（ホストＡ１００とＬＵ０－２３２間）、”０１１０”と”０００２”間の転送（ホストＢ１１０とＬＵ２－２３６およびＬＵ３－２３８間）、”０１２０”と”０００１”間の転送（ホストＣ１２０とＬＵ１－２３４間）、”０１２０”と”０００２”間の転送（ホストＣ１２０とＬＵ２－２３６およびＬＵ３－２３８間）、”０１３０”と”０００１”間の転送（ホストＤ１３０とＬＵ１－２３４間）を許可するように指定する。なお、ホストＣ１２０、ホストＤ１３０、ディスクアレイ２００はともにネットワークＢ５１０上にあるので、その間の転送はルータ３００を介することはない。そのため、ＩＰアドレス”０１２０”と”０００１”間の転送、”０１２０”と”０００２”間の転送、”０１３０”と”０００１”間の転送については、ルータ３００に許可するように指定しなくとも良い。

【００３１】ＩＰパケットの中の転送元ＩＰアドレスと転送先ＩＰアドレスを調べ、許可されていない不正な転送をフィルタリングする機能は、従来のルータが備えているパケットフィルタリングの一機能であるので、本発明において、ルータ３００には特別に新しい機能は必要なく、従来のルータを使用可能である。

【００３２】上記設定により、ホストＡ１００がＬＵ０－２３２をアクセスする際には、転送元ＩＰアドレス”０１００”、転送先ＩＰアドレス”０００”のＩＰパケットを使用する。ＩＰアドレス”０１００”と”０００”間の転送はルータ３００では許可するように設定されているので正当な転送とみなされ、同様にディスクアレイ２００内のＩＰフィルタリング手段２１６でも正当と判定され、通常のアクセス処理が行われる。

【００３３】ここでもし、ホストＢ１１０がＬＵ０－２３２にアクセスするために転送元ＩＰアドレス”０１１０”、転送先ＩＰアドレス”０００”のＩＰパケットを使用したとすると、ＩＰアドレス”０１１０”と”０００”間の転送はルータ３００では許可されていないので、不正な転送とみなされ破棄される。

【００３４】ホストＢ１１０がＬＵ０－２３２にアクセスするために転送元ＩＰアドレス”０１１０”、転送先ＩＰアドレス”０００２”のＩＰパケットを使用したとすると、ルータ３００はＩＰパケット内部のＬＵを認識できず、ＩＰアドレスしか認識しないために、この不正なパケットを通してしまうが、ディスクアレイ２００内のＩＰアドレス－ＬＵＮ対応付け手段２１４のＩＰアドレス－ＬＵＮマッピングテーブル５００においてＩＰアドレス”０００２”とＬＵ０が対応付けられていないことが判るので、ディスクアレイ２００内部でこの転送を不正な転送とみなして破棄することができる。

【００３５】以上の構成、動作により本実施形態によれば、ｉＳＣＳＩ技術でＩＰネットワークに接続されるディスクアレイにおいて、ＩＰパケット内の転送元ＩＰアドレスと転送先ＩＰアドレスの組により、従来のＬＵＮセキュリティと同等のセキュリティ機能を実現することができる。

【００３６】また、ネットワークを相互に接続するルータにおいて、同様のＩＰアドレスの組により、従来のＬＵＮセキュリティと同等のセキュリティ機能を、ディスクアレイの外部で実現することができる。

【００３７】さらに、ＬＵごとにＩＰアドレスを対応付けるということは、ホストからは複数のディスクアレイがあるのと等価に見えるということであり、多数のディスクアレイがあるのと同じ環境を１つのディスクアレイで構築できるのでより安価であり、また一元管理が可能となりディスクアレイの管理コストを下げる効果もある。

【００３８】さらに、負荷の大きいＬＵを別のインタフェースや別装置へ移行する際に、対応付けたＩＰアドレスごと移行することが可能であり、以降後もホストからは同じ環境でアクセス可能となり、以降を容易に実現できるという効果もある。

【００３９】なお、本実施例では、管理端末４００からディスクアレイ２００およびルータ３００への管理情報の転送は、ネットワークＢ５１０を介して行っているが、図６に示すようにネットワークＢ５１０ではなく、管理端末４００とディスクアレイ２００を結ぶ専用線７００および管理端末４００とルータ３００を結ぶ専用線７１０を使用して管理情報の転送を行っても良い。専用線７００と７１０はたとえばシリアル通信線などで実現できる。

【００４０】また、本実施例では、ＬＵ１－２３４はネットワークＢ５１０上のホストからしかアクセスされないが、この場合はＬＵ１－２３４に対応するＩＰアドレス”０００１”をネットワークＢ５１０上でのみ有効なローカルアドレスにすれば、ＬＵ１－２３４に関するデータ転送はルータを介して外のネットワークに出て行くことはなくなり、よりセキュリティ的に安全となる。

【００４１】また、本実施例では、ホストがイニシエータになりディスクアレイをアクセスする例で説明したが、インターネットを介した遠距離バックアップ等の為に、ディスクアレイがイニシエータになったデータ転送も考えられる。そのような場合には、バックアップ対象のＬＵにイニシエータ用のＩＰアドレスを対応付けることにより、ディスクアレイ２００から外部のネットワーク上の装置へのデータ転送においても、本実施例と同じくルータ３００上で転送ＩＰアドレスの組によるフィルタリングによってセキュリティチェックを実施できる。

【００４２】また、本実施形態では、ホストは単一のネットワークインタフェースを持っているとして説明したが、ホストが複数のネットワークインタフェースを持ち、それぞれに別のＩＰアドレスを使用する場合でも同様に実現できる。さらに、ホストが１つのネットワークインタフェースに複数のＩＰアドレスを割り付け、ＩＰアドレスごとに使用法を変える場合にも、複数のホストが存在するのと同様にして実現可能である。

【００４３】また、本実施形態では、ディスクアレイは単一のネットワークインタフェースを持っているとして説明したが、ディスクアレイが複数のネットワークインタフェースを持ち、それぞれに別の複数ＩＰアドレスを使用する場合でも同様に実現できる。

【００４４】また、本実施形態ではディスクアレイ２００にＩＰアドレス－ＬＵＮ対応付け手段２１４およびＩＰフィルタリング手段２１６を設けたが、これらを設けず、該当機能をＭＰＵ２２４およびメモリ２２２にて実現しても良い。

【００４５】

【発明の効果】以上述べたように、本発明によれば、ディスクアレイのネットワークインタフェースに複数のＩＰアドレスを保持できる手段と、ディスクアレイ内部のＬＵとＩＰアドレスを対応付ける手段と、ＩＰパケットの転送元ＩＰアドレスと転送先ＩＰアドレスの組を見て転送をフィルタリングできる手段を設け、ホストとＬＵの転送はＬＵに対応付けられたＩＰアドレスを転送先ＩＰアドレスに指定して転送することとし、管理端末がＩＰアドレスとＬＵＮのマッピングおよびどの転送元ＩＰアドレスと転送先ＩＰアドレスの組の転送が許可されるかの設定を行うことにより、ディスクアレイおよびルータにて転送元ＩＰアドレスと転送先ＩＰアドレスの組を調べることで不正な転送を破棄できるようになり、ディスクアレイおよびディスクアレイの外部のルータ上で従来のＬＵＮセキュリティと同等のセキュリティを実現可能であるという効果が得られる。

【図面の簡単な説明】

【図１】本発明のネットワーク構成図である。

【図２】本発明におけるディスクアレイの内部ブロック図である。

【図３】本発明における管理端末の内部ブロック図である。

【図４】ＩＰアドレスとＬＵＮのマッピングテーブルを示す図である。

【図５】ホストがアクセス可能なＬＵのテーブルを示す図である。

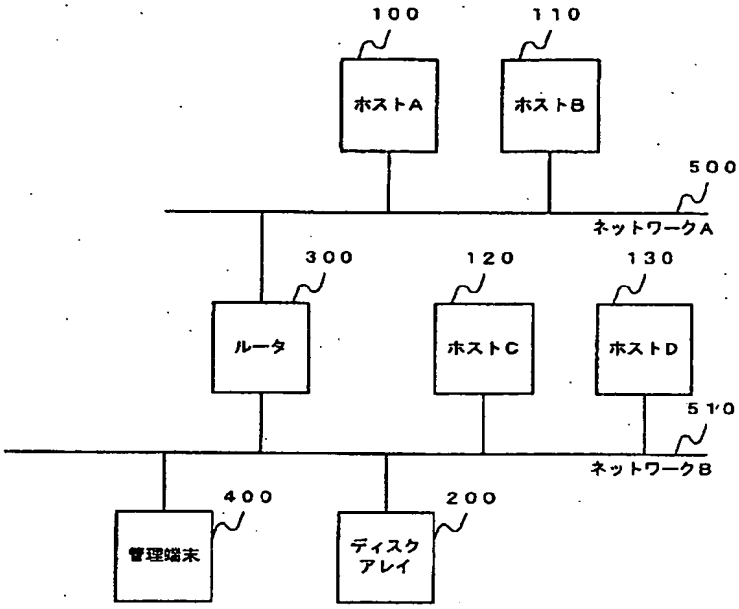
【図６】別構成のネットワーク構成図である。

【符号の説明】

１００…ホストＡ、１１０…ホストＢ、１２０…ホストＣ、１３０…ホストＤ、２００…ディスクアレイ、３００…ルータ、４００…管理端末、２１０…ネットワークインタフェース、２１２…複数ＩＰアドレス保持手段、２１４…ＩＰアドレス－ＬＵＮ対応付け手段、２１６…ＩＰフィルタリング手段。

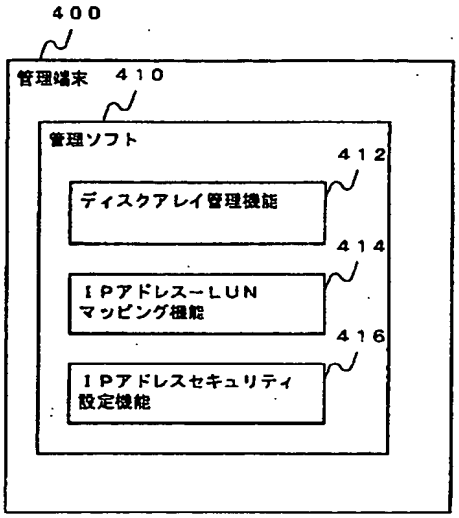
【図１】

図　1



【図３】

図　3



【図４】

図　4

IPアドレス－LUNマッピングテーブル
500

510 IPアドレス	520 LU番号
0000	LU0
0001	LU1
0002	LU2
0002	LU3

【図５】

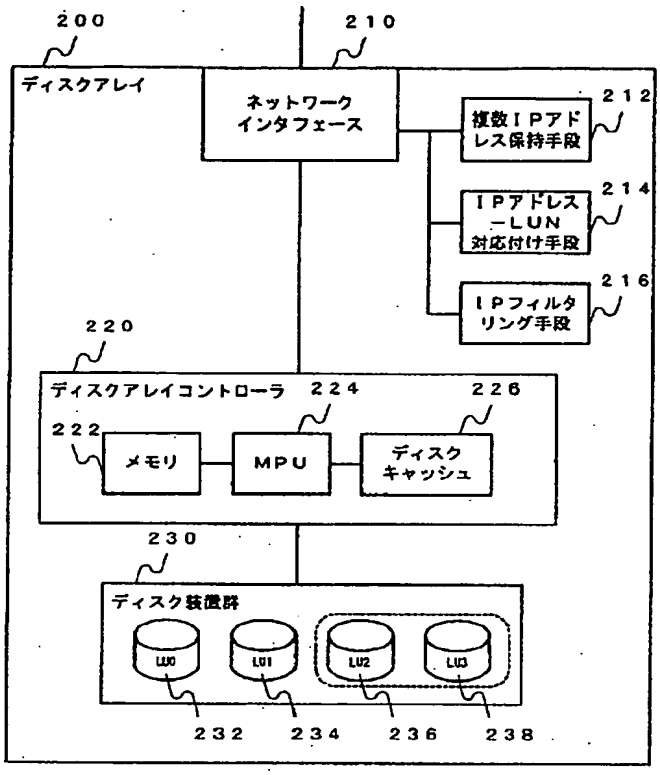
図　5

アクセス可能LU対応テーブル600

610 ホスト	620 ホストIPアドレス	630 アクセス可能LU	640 LU対応IPアドレス
ホストA	0100	LU0	0000
ホストB	0110	LU2	0002
ホストB	0110	LU3	0002
ホストC	0120	LU1	0001
ホストC	0120	LU2	0002
ホストC	0120	LU3	0002
ホストD	0130	LU1	0001

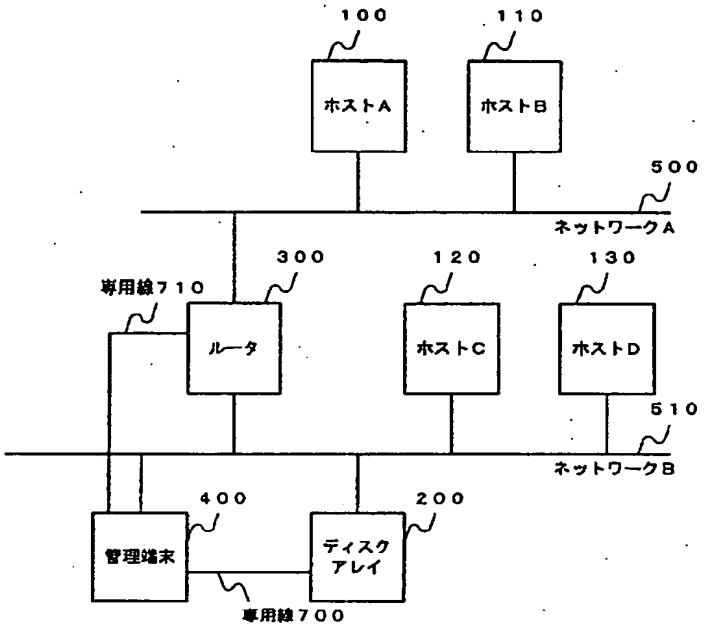
【図２】

図 2


200
210
ディスクアレイ
ネットワーク
インタフェース
212
複数ＩＰアドレス保持手段
214
ＩＰアドレス－LUN対応付け手段
216
ＩＰフィルタリング手段
220
ディスクアレイコントローラ
224
226
222
メモリ
MPU
ディスクキャッシュ
230
ディスク装置群
LU0
LU1
LU2
LU3
232
234
236
238

【図６】

図　６



フロントページの続き

(72)発明者　味松　康行
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　松並　直人
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　村岡　健司
神奈川県小田原市国府津2880番地　株式会社日立製作所ストレージ事業部内

Ｆターム(参考)　5B017 AA07 BA01 CA07
5B065 BA01 CA30 PA12